SYNOPSYS®

Black Duck

Product configurations and modules

Black Duck provides complete control over open source risk, regardless of your organization's size or budget

Overview

Black Duck® software composition analysis (SCA) can be implemented in two out-of-the-box configurations—Security Edition and Professional Edition. Black Duck Binary Analysis and the cryptography module can be added to either edition to provide greater insight into your application risk posture and enhanced control over your open source and third-party software consumption.

Black Duck Security Edition

Automatically identify and remediate open source risks throughout your entire SDLC

Black Duck Security Edition can run either a full dependency scan during a build or a fast scan using the Code Sight™ IDE plugin to provide visibility into the open source security risks in your applications. Black Duck automatically discovers open source components in your applications, and also provides a complete open source Bill of Materials (BOM) for your software projects, giving you critical insight into any known vulnerabilities, as well as the license and code quality risks affecting your applications.

- **Vulnerability mapping** identifies any security risks associated with the open source components in your applications at any point in your software development life cycle (SDLC).
- **Vulnerability monitoring and alerting** automatically monitors for new vulnerabilities against inventoried open source components. It also helps accelerate remediation by instantly alerting security and development teams with detailed and actionable information.
- **Black Duck Security Advisories (BDSAs)** provide notifications of vulnerable open source component versions, including detailed descriptions, exploit profiles, severity scoring, impact analysis, and detailed remediation guidance that security experts and developers alike can understand.
- **License risk identification** safeguards sensitive intellectual property and helps avoid litigation by identifying the open source licenses that apply to the components in your applications. You can view license terms and obligations, automatically generate notice files, and define your own custom policy and let Black Duck handle the enforcement.
- **Operational risk metrics** mitigates the risk of higher support and remediation costs for your development teams by identifying out-of-date component versions or those with limited project activity and community engagement.
- **Rapid Scan** instantly analyzes open source dependencies for vulnerabilities and policy violations before code is built or merged into release branches.

- **Policy configuration** lets you manage and mitigate risk throughout the SDLC. Structure policies for secure and compliant open source consumption and usage, and automate policy violation notifications for faster enforcement and remediation.
- **DevOps integrations** automate open source discovery and provide critical risk insight to the teams who need it, when they need it. Integrations are available for CI/CD tools, package managers, IDEs, container platforms, code repositories, issue trackers, and application security suites.
- **Black Duck KnowledgeBase** is the industry's largest database of open source project, vulnerability, and license data. Map your BOM to more than 15 years of data, 30% more vulnerabilities than are tracked in the National Vulnerability Database (NVD), and over 2,750 unique licenses.

Black Duck Professional Edition

Completely manage open source risk and consumption in your SDLC

Black Duck Professional Edition gives teams the tools they need to fully manage open source risks across their applications and containers. Professional Edition includes all the capabilities of Black Duck Security Edition, plus Black Duck's advanced security and license compliance capabilities. Regardless of how large your organization or development team is, or what languages and technology you're employing in your applications, Black Duck scales to meet your unique business needs and provides the most complete risk picture on the market.

Multifactor open source discovery

Not all open source is explicitly declared or included in its original form, but it still carries risk. Black Duck identifies all open source components in your applications, modified or unmodified, partial or whole, via a combination of discovery techniques.

- **Dependency analysis** tracks declared components and dependencies
- **Code print analysis** finds undeclared, modified, and partial components, even in languages that don't use package managers, like C/C++
- **Snippet matching** identifies snippets of open source embedded in your code
- **Binary analysis** detects open source in virtually any compiled software, firmware, or installer format without access to source code or build systems
- **Custom component detection** uses string searching and code printing to find non-open-source, internal, or third-party commercial components

Advanced license compliance

Protect intellectual property and mitigate the risk of open source license noncompliance with greater insight into license obligations and attribution requirements. Black Duck provides:

- Identification and analysis of all applicable licenses beyond those declared
- Automated generation of customizable open source software reports at the project/release level
- Full texts for the most popular open source licenses
- The ability to view license responsibilities and confirm that license commitments have been met

Snippet analysis identifies small sections of code originating from open source components that carry the same license obligation as those components. Black Duck enables you to:

- View code snippet matches highlighted in the component source, augmenting the accuracy of your open source BOM
- Perform a full codebase scan or accelerate your analysis with a delta scan, examining only the files that have changed
- Evaluate and triage matches by license risk, matched component version release data, and prevalence
- Review key snippet data, including matched component name and version, component license, path, percentage of scanned code matched to component file, and release date
- Confirm, flag, or ignore potential matches en masse with bulk edit capabilities

Additional Black Duck solutions

Black Duck is available with additional security enhancements to further your open source risk management capabilities. Both Black Duck Binary Analysis (BDBA) and the cryptography module can be added to Black Duck Security Edition or Professional Edition.

Black Duck Binary Analysis

Modern software is a patchwork of open source software, commercial code, and internally developed components, and the tendency to defer accountability throughout today's complex software supply chain exposes you to significant risk. Vulnerable open source components in your applications are weak links in the supply chain, providing a viable point of entry for attackers. Take steps to identify the risks in the software libraries, executables, and vendor-supplied binaries in your codebase. Black Duck Binary Analysis helps you:

- Analyze virtually any compiled software, firmware, mobile application, or installer format without access to source code
- Create a detailed BOM of vulnerable open source components, including version, location, license, and known vulnerabilities
- Use data from the NVD, including CVSS 2.0 and 3.x metrics, to rank vulnerabilities for remediation
- Access detailed vulnerability descriptions, links to vendor advisories, patches, and more
- Receive automatic alerts about new vulnerabilities in previously scanned software
- Identify declared open source licenses and any potential risk of noncompliance
- Use the REST API to accelerate and automate essential risk mitigation and remediation tasks
- Identify potential sources of sensitive data leakage that might be in a software package
- Gain insight into requested permissions for binary code types where relevant, such as in Android and iOS apps
- Identify components that have been compiled without exploit mitigation mechanisms or that contain dangerous execution configurations

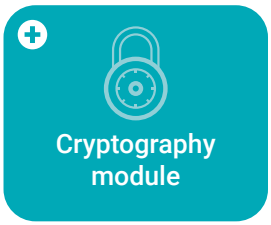
Cryptography module

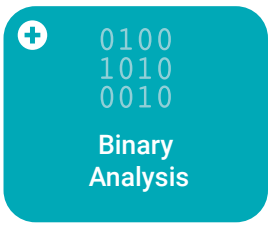
This module supports data security initiatives and regulations around the legal export of cryptography by tracking the cryptographic algorithms in the open source components in your applications and identifying weak cryptography or obsolete hashing mechanisms.

The Black Duck cryptography module provides:

- Identification of encryption algorithms found in each open source component version
- Detailed cryptography data including key length, originator, licensing, and patent information
- Indication of weak encryption

	Security Edition	Professional Edition
Scanning	Dependency, rapid	Multifactor scanning
Vulnerability info	BDSA	BDSA
License info	Basic	Advanced
Policy	●	●
Monitoring	●	●
Reporting	●	●
Integrations	All	All
Auto-remediation	●	●
Reachability	●	●
Containers	●	●
On-prem options	●	●





Black Duck | Source and Package Manager Scanning

■ Black Duck only
✖ BDBA only

Scanning

Languages

- C
- C++
- C#
- Clojure
- Erlang ■
- Golang
- Groovy
- Java
- JavaScript ■
- Kotlin
- Node.js ■
- Objective-C
- Perl ■
- Python ■
- PHP ■
- R ■
- Ruby
- Scala
- Swift ■
- .NET Cloud technologies

Package managers

- NuGet ■
- Hex ■
- Vndr ■
- Godep ■
- Dep ■
- Maven ■
- Gradle ■
- Npm ■
- CocoaPods ■
- Cpanm ■
- Conda ■
- Pear ■
- Composer ■
- Pip ■
- Packrat ■
- RubyGems ■
- SBT ■
- Bazel
- Cargo
- C/C++ (Clang)
- GoLang
- Erlang/Hex
- Rebar
- Python
- Yarn
- Yocto

BDBA package manager support

- Distro-package-manager: Leverages information from a Linux distribution package manager database to extract component information
- The remaining four methods are only applicable to Java bytecode:
  - pom: Extracts the Java package, group name, and version from the pom.xml or pom.properties files in a JAR file
  - manifest: extracts the Java package name and version from the entries in the MANIFEST.MF file in a JAR file
  - jar-filename: Extracts the Java package name and version from the jar-filename
  - hashsum: Uses the sha1 checksum of the JAR file to look it up from known Maven Central registered Java projects

Binary formats

- Native binaries
- Java binaries
- .NET binaries
- Go binaries

Compression formats

- Gzip (.gz)
- bzip2 (.bz2)
- LZMA (.lz)
- LZ4 (.lz4) ✖
- Compress (.Z)
- XZ (.xz)
- Pack200 (.jar)
- UPX (.exe)
- Snappy
- DEFLATE
- zStandard (.zst) ✖

Archive formats

- ZIP (.zip, .jar, .apk, and other derivatives)
- XAR (.xar) ✖
- 7-Zip (.7z)
- ARJ (.arj)
- TAR (.tar)
- VM TAR (.tar) ✖
- cpio (.cpio)
- RAR (.rar)
- LZH (.lzh) ✖
- Electron archive (.asar) ✖
- DUMP

Installation formats

- Red Hat RPM (.rpm)
- Debian package (.deb)
- Mac installers (.dmg, .pkg)
- Unix shell file installers (.sh, .bin)
- Windows installers (.exe, .msi, .cab)
- vSphere Installation Bundle (.vib) ✖
- Bitrock Installer ✖
- Installer generator formats that are supported:
  - 7z, zip, rar self-extracting .exe ✖
  - MSI Installer ✖
  - CAB Installer ✖
  - InstallAnywhere ✖
  - Install4J ✖
  - InstallShield ✖
  - InnoSetup ✖
  - Wise Installer ✖
  - Nullsoft Scriptable Install System (NSIS) ✖
  - WiX Installer ✖

Firmware formats

- Intel HEX ✖
- SREC ✖
- U-Boot ✖
- Arris firmware ✖
- Juniper firmware ✖
- Kosmos firmware ✖
- Android sparse file system ✖
- Cisco firmware ✖

File systems / disk images

- ISO 9660 / UDF (.iso) ✖
- Windows Imaging ✖
- ext2/3/4 ✖
- JFFS2 ✖
- UBIFS ✖
- RomFS ✖
- Microsoft Disk Image ✖
- Macintosh HFS ✖
- VMware VMDK (.vmdk, .ova) ✖
- QEMU Copy-On-Write (.qcow2) ✖
- VirtualBox VDI (.vdi) ✖
- QNX—EFS, IFS ✖
- NetBoot image (.nbi) ✖
- FreeBSD UFS ✖

Container formats

- Docker

Black Duck | Integrations

Cloud technologies

Cloud platforms
- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure
- Pivotal Cloud Foundry

Container platforms
- Docker
- OpenShift
- Pivotal Cloud Foundry
- Kubernetes Package managers

Databases
- PostgreSQL

DevOps tools

IDEs
- Eclipse
- Visual Studio IDE
- IntelliJ IDEA
- WebStorm
- PyCharm
- RubyMine
- PhpStorm
- VS Code
- Android Studio

Continuous integration
- Jenkins
- TeamCity
- Bamboo
- Team Foundation Server
- Travis CI
- CircleCI
- GitLab CI
- Visual Studio Team Services
- Concourse CI
- AWS CodeBuild
- Codeship
- Azure DevOps
- GitHub Actions
- OpenShift

Workflow and notifications
- Jira
- Slack
- Email
- SPDX
- Azure Boards
- Microsoft Teams

Binary and source repositories
- Artifactory
- Nexus

Application security suites
- IBM AppScan
- Micro Focus Fortify
- SonarQube
- ThreadFix
- Cybric
- Code Dx
- Fortify
- ZeroNorth

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com